Subject	Date	Policy #
Employee Account Policy	September 2020	ITS-4.2
	Application	**Supersedes**
	ITS Security	ITS-4.1
	Distribution	
	All Departments	
Recommended	**Approved**	
Preston D. Marx, VP Information Systems	James I. Marshall, Administrator - CEO	

1.0 Purpose

This policy defines the standards and procedures for the creation, maintenance and deletion of employee user accounts.

2.0 Scope

The policy applies to all solution accounts managed by Uintah Basin Healthcare ITS. Accounts include: AD Domain accounts, email accounts, EMR accounts and all other managed solutions requiring account maintenance.

3.0 Policy

Overview

Uintah Basin Healthcare believes that the use of individual user accounts is essential to promote and enforce user accountability for activity conducted. Employees are required to keep their accounts secure and protected as any activity performed under their account will be attributed to them.

Uintah Basin Healthcare incorporates least privilege access models when protected health information is involved, such that the amount of information should be limited to that which is absolutely necessary to accomplish the intended purpose of the use or disclosure.

Manager Responsibilities

The authorization of access to UBH resources is the responsibility of the department manager. Managers should be familiar with job functions and ensure proper access is assigned. The ITS team works with the manger to conduct semi-annual audits of personnel security and make changes as needed. The ITS team maintains a record of all active users, their credentials and any access

EXHIBIT 5

granted. The ITS team shall not grant or modify user access to protected health records unless given proper authorization from the manager.

Account Creation

All employees are issued an active directory account and corresponding corporate e-mail account when hired. Employees are encouraged to protect and use this account for all terminal access and communication.

As a part of the new employee packet the manager assigns and authorizes employee access to other ITS supported solutions. All forms must be filled out, signed and returned to ITS before any access is granted.

All accounts should adhere to the Uintah Basin Healthcare password policy which sets rules for password retention, length and safeguarding.

Access to Electronic Personal Health Information (ePHI)

It is mandatory that all access to systems containing PHI are assigned to unique user IDs (including not sharing accounts, ensuring all user IDs are associated with a person). After HR has submitted a ticket for the active directory and email accounts, the employee's manager must submit an osTicket for additional access into any EMR accounts (ie. Cerner, Clarity, Philips Intellispace, T-Systems, etc.) which contain ePHI.

Managers will include a “Like” User for ITS to copy the account after for specific access into each module.

After the account is set up, ITS will reply in osTicket the User's credentials to the User's Manager.

Please refer to ITS Account Procedure for exact steps in creating EMR accounts.

Employee Account Modification

Human Resources and the ITS team must be notified of any employee transfer or change of duties that would necessitate modification of employee access to UBH resources. Manager approval is required before any changes are made.

Account modification temporarily for unexpected shift work or application testing is permissible and must be coordinated between the manager and ITS.

Employee Account Termination

Human Resources and the ITS team must be notified of any employee termination. Unless previously communicated, all access to UBH resources are immediately disabled upon termination. Active Directory accounts and their associated e-mail account are retained in a disabled status for 30 days; after which the account is deleted. Cerner accounts remain in the system indefinitely for auditing purposes but should remain inactive unless employment resumes.

For security purposes, any member of the ITS department with system-level access, regardless of the reason for job termination, will be immediately dismissed and user accounts disabled.

Violations

Uintah Basin Healthcare takes user access seriously. Anyone found doing activities that are outside the scope of an employee' duties or misusing access privileges will be subject to corrective action up to and including termination.

Employee access controls are intended to be a safeguard to protect Uintah Basin Healthcare and the employee from unauthorized access. However, the onus of user access and activity reside with the individual employee. If necessary, Uintah Basin Healthcare also reserves the right to advise appropriate legal officials of any illegal violations.